

REMARKS/ARGUMENTS

Claims 1 through 11 are pending and have been examined. Claims 1 and 6 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter. Claim 6 was objected to because it contained an informality, namely an unidentified acronym. Claim 1 was rejected under 35 U.S.C. 103(a) as being obvious over U.S. Publication No. 2003/0120615 (“Kuo”) in view of U.S. Patent No. 5,724,424 (“Gifford”). Claims 2 through 11 were rejected under 35 U.S.C. 103(a) as being obvious over Kuo and Gifford in view of U.S. Publication No. 2001/0034720 (“Armes”).

Applicants have amended claim 6 to correct the informality objected to by the Examiner. This amendment was made to clarify the scope of claim 6, and has not in any way narrowed the scope of claim 6 from what it was previously. Applicants respectfully request withdrawal of the Examiner’s objection to claim 6.

For the reasons explained below, Applicants respectfully request reconsideration of the Examiner’s rejections of claims 1 through 11.

I. Claims 1 and 6 Are Directed to Statutory Subject Matter

In paragraph 2 of the Office Action, the Examiner rejected claims 1 and 6 as being directed to non-statutory subject matter, asserting that claims 1 and 6 are directed to nothing more than the manipulation of an abstract idea, and have no practical application in the technological arts. *See* Feb. 26th Office Action at p.2. The Applicants respectfully disagree, and earnestly request withdrawal of this rejection.

Section 2106, subsection IV of the Manual of Patent Examining Procedure (“MPEP”) addresses the question of whether a claimed computer-related invention is directed to statutory subject matter. In paragraph (A)(2)(b)(ii) of that subsection, the MPEP states that for a process that manipulates an abstract idea or performs a purely mathematical algorithm to be statutory, “the claimed process must be *limited to a practical application* of the abstract idea or mathematical algorithm in the technological arts . . .” (emphasis supplied) (citations omitted). The MPEP goes on to explain that “a claim is limited to a practical application when the method,

as claimed, produces a concrete, tangible and useful result; *i.e.*, the method recites a step or act of producing something that is concrete, tangible and useful . . . For example, a computer process that simply calculates a mathematical algorithm that models noise is non-statutory. *However a claimed process for digitally filtering noise employing the mathematical algorithm is statutory . . .*" (emphasis supplied) (citations omitted).

Under this standard, claims 1 and 6 are each directed to statutory subject matter. Each of the presently pending claims recites a method of conducting an electronic transaction over a public communications network employing a particular computer algorithm. Claims 1 and 6 each recites a process that produces something "concrete, tangible and useful" – an electronic transaction over a public communications network – using an computer algorithm. Far from being directed to non-statutory subject matter, claims 1 and 6 cover a process for producing a useful and tangible result using an algorithm in a manner that is precisely analogous to the example of a statutory computer-related process given in Section 2106 of the MPEP.

For these reasons, Applicants respectfully request that the Examiner withdraw the rejection of claims 1 and 6 under Section 101.

II. The Combination of Kuo and Gifford Fails to Establish a Prima Facie Case of Obviousness With Respect to Claim 1

In paragraphs 4 and 5 of the Office Action, claim 1 was rejected as being obvious over Kuo in view of Gifford. Applicants respectfully request reconsideration of this rejection.

Claim 1 is independent and requires, among its limitations, several limitations that use a message authentication code, or "MAC," to authorize and verify a transaction. More particularly, claim 1 requires, among its limitations, generating a secret key associated with a payment account number and using the secret key to generate a MAC specific to the transaction; generating an authorization request message including the MAC; forwarding the authorization request message over said payment network to said check site for verifying the authenticity of the MAC; and verifying the MAC by the check site using the secret key.

It is well known to those of ordinary skill in the art that a MAC is a key-dependent one-way hash function. As is explained in Applied Cryptography, Second Edition, by Bruce

Schneier, which is an authoritative reference on computer-based cryptography, a hash function is a function, mathematical or otherwise, that takes a variable-length input string (called a pre-image), and converts it into a fixed-length output string (called a hash value). A one-way hash function is a hash function that works in one direction. Using a one-way hash function it is easy to compute a hash value from the pre-image, but difficult to generate a pre-image that hashes to a particular value. The hash function itself is public; there is no secrecy to the process. The security of the one-way hash function is its “one-wayness.” Given a hash value generated by a one-way hash function, it is computationally unfeasible to find a pre-image that hashes to that value.

A MAC is, as was stated previously, a one-way hash function with the addition of a secret key. That is to say, the hash value generated using a MAC is a function of both the pre-image and the secret key. The difference between a MAC and an ordinary one-way hash function is that only someone with the secret key can verify the hash value.

Kuo, which is the primary reference that the Examiner relies on, neither discloses nor suggests the limitations of (i) generating a secret key associated with a payment account number and using the secret key to generate a MAC specific to the transaction, (ii) generating an authorization request message including the MAC, or (iii) forwarding the authorization request message over the payment network to the check site for verifying the authenticity of the MAC, as independent claim 1 requires. In fact, Kuo does not disclose or suggest the use of MACs at all. Rather, Kuo describes the use of key pairs for authorization and verification of transactions, with one key of the pair – not a MAC – being used as the authentication code. *See Kuo, para. [0055].*

Gifford was not cited by the Examiner as curing the above-mentioned deficiencies of Kuo. Rather, the Examiner cited Gifford solely as disclosing the limitation of claim 1 requiring verification of the MAC by the check site using the secret key. In any event, Gifford neither cures the deficiencies of Kuo with respect to claim 1, nor does it disclose a check site that verifies a MAC using the secret key.

Gifford is directed to various methods for creating what it refers to as “authenticators.” *See Gifford, col. 5, ln. 30 – col. 11, ln. 50.* The only authenticators seemingly addressed in

Gifford that are hash values generated using secret keys (like the MACs required by claim 1) are those that are created using a smart card. *See* Gifford, col. 10, ln. 54 – col. 11, ln. 7. More particularly, Gifford is directed to the use of a smart card containing a secret key to create a digital signature of a payment order. *See* Gifford, col. 10, lns. 62 – 66.

Gifford never discloses nor suggests that the secret key is associated with a payment account number, or that an authorization request message including the MAC is forwarded over the payment network to a check site for verifying the authenticity of the MAC. Thus, Gifford does not cure the above-described deficiencies in Kuo, and the combination of Kuo and Gifford cited by the Examiner fails to recite at least these limitations of independent claim 1.

For these reasons, Applicants respectfully request that the rejection of independent claim 1 as being obvious over Kuo in view of Gifford be withdrawn.

III. The Combination of Kuo, Gifford and Armes Fails to Establish a Prima Facie Case of Obviousness With Respect to Dependent Claims 2 through 5

In paragraph 5 of the Office Action, claims 2 through 5 were rejected as being obvious over the combination of Kuo, Gifford and Armes. Applicants respectfully request reconsideration of this rejection.

Claims 2 through 5 depend from, and include all of the limitations of, independent claim 1. As was explained above, the combination of Kuo and Gifford is deficient with respect to a number of limitations of independent claim 1. The Examiner, however, did not cite Armes as disclosing any of the limitations of claim 1. Rather, Armes was cited as disclosing other limitations that are recited solely by dependent claims 2 through 5. Thus, the combination of Kuo, Gifford and Armes remains deficient with respect to claims 2 through 5, and Applicants accordingly request that the rejection of claims 2 through 5 be withdrawn.

IV. The Combination of Kuo, Gifford and Armes Fails to Establish a Prima Facie Case of Obviousness With Respect to Independent Claim 6

In paragraph 7 of the Office Action, independent claim 6 was rejected as being obvious over the combination of Kuo, Gifford and Armes. Applicants respectfully request reconsideration of this rejection.

Claim 6 includes a number of limitations that include the generation and verification of a MAC. More particularly, claim 6 requires generating a per-card key associated with said payment account number; generating a message authentication code (MAC) using said per-card key; generating a MAC verification request including said payment account number and said MAC; verifying said MAC; and based on said verification, creating an expected transaction sequence number (ETSN) for said MAC.

As was previously explained in connection with claim 1, Kuo, which is the primary reference that the Examiner relies on, neither discloses nor suggests the use of MACs at all. Rather, Kuo describes the use of key pairs for authorization and verification of transactions, with one key of the pair – not a MAC – being used as the authentication code. *See Kuo, para. [0055].* Thus, Kuo fails to disclose or suggest any of the above-described limitations that include the generation and verification of a MAC.

Gifford does not cure these deficiencies in Kuo. Neither the portions of Gifford cited by the Examiner, nor any other portions of Gifford, discloses creating an expected transaction sequence number (ETSN) for the MAC based on the verification of the MAC. The Examiner asserts that Gifford discloses this limitation in col. 11, lns. 33 – 44. Applicants respectfully disagree. What is disclosed in that portion of Gifford is a sixth method for authenticators, in which the user is queried for a transaction identifier that is the next string from a physical list of one-time authorization strings. The transaction identifier is an authorization string that is checked against a database of strings. The database can hold for each sender a list of random authorizations strings, or can hold a sender specific secret key that was used to generate the list of authentication strings. Nowhere does Gifford disclose or suggest that this transaction number is created based on the verification of the MAC, as is required by independent claim 6.

Armes is not cited by the Examiner as curing the above-mentioned deficiencies in Kuo and Gifford. Rather, Armes is cited solely as disclosing routing the second MAC to the check site based on the BIN associated with the check site. In any event, there is no discussion whatsoever in Armes of using MACs to authenticate and/or verify transactions, and thus the combination of Gifford and Kuo with Armes remains deficient with respect to independent claim 6 for the reasons described above.

Applicants accordingly request withdrawal of the rejection of claim 6 as being obvious over Kuo, Gifford and Armes.

V. The Combination of Kuo, Gifford and Armes Fails to Establish a Prima Facie Case of Obviousness With Respect to Independent Claims 7 through 11

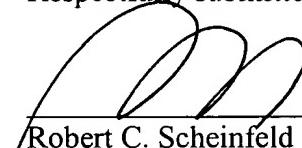
Claims 7 through 11 depend from, and include all of the limitations of independent claim 6. The Examiner has rejected claims 7 through 11, however, based on the same art that was cited against claim 6 – namely Kuo, Gifford, and Armes. This combination is thus deficient with respect to claims 7 through 11 as well, for the same reasons discussed above in connection with claim 6.

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 7 through 11 as being obvious over Kuo, Gifford and Armes.

VI. Conclusion

For at least the reasons set forth above, Applicants respectfully submits that all the presently pending claims are in condition for immediate allowance. In the event that the present application is not deemed to be in condition for allowance, the Examiner is invited to contact the undersigned in an effort to advance the prosecution of this application.

Respectfully submitted,



Robert C. Scheinfeld
PTO Reg. No. 31,300
Attorney for Applicant
(212) 408-2500